REMARKS

Reconsideration of the above-identified application in view of the amendments above and the remarks following is respectfully requested.

Claims 1-47 are in this case.

Claims 1-2,7,9-13 have been rejected under 35 U.S.C. §102(b) as anticipated by Hulme ("Cryptography" 1899). and claims 1-2,6 have been further rejected under §102(b) as anticipated by British War Office ("Manual of Cryptography").

Claims 3-4 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Hulme in further view of Novaes (U.S. 6,460,068).

Claim 5 is rejected under 35 U.S.C. §103(a) as being unpatentable over Hulme and Novaes (U.S. 6,460,068) and in further view of Hoffberg et. al (US 5,773,357).

Claim 8 has been rejected as being unpatentable based on Hulme and a statement by Examiner of "obviousness" by official notice.

Claims 14-15 have been rejected as unpatentable over Hulme in further view of Menezes et al. ("Handbook of Applied Cryptography").

Claims 16-19 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Hulme and Menezes et al. and in further view of Sasich et al (U.S. 6,661,904).

Claims 20-21 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Hulme, Menezes et al. and Sasich et al (U.S. 6,661,904) in further view of Bocionek et al. (US 6,301,360) and Schneier ("Applied Cryptography").

Claims 22-24 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Hulme in further view Sasich et. al (U.S. 6,661,904)

Claim 25 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Hulme, Sasich et al (U.S. 6,661,904) and Schneier ("Applied Cryptography").

Claim 26 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Hulme, Sasich et al (U.S. 6,661,904), Schneier ("Applied Cryptography") in further view of Bocionek et al. (US 6,301,360) .

Claims 1- 27 are hereby canceled without prejudice and are replaced by new claims 28-47. Claims 28-47 do not introduce any new material.

Objections to the Drawings

The Examiner has objected to the drawings because labeling failed to comply with 37 CFR 1.184(u)(1). Applicant has submitted amended drawing sheets including Figures labeled as 2A, 2B, 3A and 3B. Applicant respectfully submits that the drawings are now free from the informality mentioned by the Examiner.

Rejections under § 102(b)

Claims 1-2,7,9-13 have been rejected under 35 U.S.C. §102(b) as anticipated by Hulme ("Cryptography" 1899). and claims 1-2,6 have been further rejected under §102(b) as anticipated by British War Office ("Manual of Cryptography").

By way of introduction, after careful review of Examiner's rejections, Applicant wishes to point out that Hulme does not disclose a "method for scrambling data according to a map". An accurate term for Hulme's method is "masking" data because the letters of Hulme's message remain in order, only the message is masked and interspersed with letters not included in the message. "Scrambling" data implies changing order or "shifting" data in addition to "masking". Hence, referring to claim 1, Hulme does not disclose random scrambling or shifting of data according to a map. Moreover, Hulme does not disclose "a map required to unscramble said scrambled

units of data" because the data in Hulme's disclosure is not scrambled but masked. Nor does Hulme disclose "scrambled units of data not readable without the map". According to Hulme's disclosure the units of data, i.e. individual groups of letters are readable.

Furthermore, British War Office did not disclose "random scrambling of data according to a map". British War Office discloses alphabetic ciphers in which a previously determined parameter, *e.g.* two dimensional position or an integral number, is associated in one-to-one correspondence with each letter of the alphabet. A one-to -one correspondence is not a pure "random map" as described in the present application by for instance by randomly "moving the mouse or other pointing device" (page 9 lines 7-8)

Rejections under § 103(a)

By way of introduction, Applicant submits that the "masking" of Hulme, if combined with other steps or elements of the present invention would be inoperable, because "masking" according to Hulme requires excessive memory storage to be an effective data protection technique, perhaps up to ten times the storage required by the computerized information prior to protection according to the present invention. The present invention using "fragmenting and scrambling" does not require use of excessive storage, i.e. significantly more than the computerized information prior to protection.

Parenthetically, although Applicant believes that claim 1 is in condition for allowance thereby necessarily rendering claims 2-21 (dependent claims) also allowable, for completeness of the record, the Applicant wishes to submit brief comments regarding dependent claims.

Claims 3-4 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Hulme in further view of Novaes (U.S. 6,460,068). Applicant respectfully submits that Novaes (US 6,460,068) is in the field of testing applications and is not analogous prior art as is required to rely on a reference under 35 U.S.C. 103. For a case of "unobviousness", citing MPEP 2141.01(a), "the reference must be either in the field of Applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned."

Claim 5 is rejected under 35 U.S.C. §103(a) as being unpatentable over Hulme and Novaes (U.S. 6,460,068) and in further view of Hoffberg et al. (US 5,773,357). Applicant respectfully points out that Hoffberg et al. (as is Novaes) is not analogous prior art according to MPEP 2141.01(a) as cited above. Hoffberg is in the field of human interface devices and not pertinent to the problem of the present invention.

Claim 8 has been rejected as being unpatentable based on Hulme and a statement by Examiner by official notice that it would have been obviousness to one skilled in the art to divide the file into fragments before or after the data are scrambled. Applicant respectfully submits that "dividing a file into fragments and scrambling" is not "commonly known" in prior art data protection techniques such as encryption techniques and is not described in classic books such as "Applied Cryptography". Citing from MPEP 2144.03:

> It would not be appropriate for the examiner to take official notice of facts without citing a prior art reference where the facts asserted to be well known are not capable of instant and unquestionable demonstration as being well-known. For example, assertions of technical facts in the areas of esoteric technology or specific knowledge of the prior art must always be supported by citation to some reference work recognized as standard in the pertinent art.

Applicant respectfully requests from Examiner to support the "official notice with a prior art reference. Moreover, Applicant further submits that "to allow the fragments to take separate paths to a destination" is not taught nor suggested in prior references. Nor is the motivation suggested by Examiner consistent with or suggested in the present application. The present application uses "fragmenting and scrambling data to protect data, *e.g.* for instance stored data, not necessarily for communications and therefore fragmenting for the purpose of transmitting different fragments to distinct destinations is not relevant to "the nature of the problem to be solved" (MPEP 2143.01) and therefore would not be suggested to those of ordinary skill in the art.

Claims 14-19 have been rejected as unpatentable over Hulme in further view of Menezes et al. ("Handbook of Applied Cryptography"). Applicant submits that Menezes et al. (p.497) does not disclose keys in sequential order, each key based on a a random map. Menezes et al. (page 497) describes a prior art case of symmetric encryption using multiple symmetric keys. As an example of Menezes et al. , Alice is sending secret messages to Bob using a symmetric key. Eve is eavesdropping on the messages in order to obtain the key. Because Eve may succeed, the key must be changed frequently. Menezes et al. describe a conventional case in which a stack of symmetric keys is shared between Alice and Bob each key of the stack generated by an algorithm previously defined and shared by Alice and Bob. In principle, Eve on obtaining by eavesdropping a large number of the keys, may be able to determine the algorithm used to generate the keys. In the present invention, the keys are generated based on one or more randomly generated maps, not on an algorithm and therefore with the present invention it would be impossible for Eve to generate subsequent keys based on obtaining by eavesdropping a large number of sequential keys.

Claims 16-19 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Hulme and Menezes et al. and in further view of Sasich et al (U.S. 6,661,904). Regarding claim 16, Applicant respectfully traverses Examiner's statement that Sasich et al. (column 6 lines 25-29) teaches sequential keys which include information about a location for storing data and a portion of a random map both for sequentially unscrambling the data including the location of the next set of data. Sasich (column 6 lines 25-29) doesn't describe sequential unscrambling of data in which a part of the unscrambled data includes location information for the next set of data. Sasich (column 6 lines 25-29) addresses the problem of embedding large amounts of data in an image without degrading base the image and therefore suggests using large images or multiple linked images.

While continuing to traverse the Examiner's rejections, and without in any way prejudicing the patentability of the rejected claims, the Applicant has, in order to expedite the prosecution, chosen to amend the claims thereby rendering moot Examiner's rejections.

Applicant wishes to reiterate "unexpected results" as discussed in the present application (page 30 lines 6-10, 14-15). "The present invention is useful for producing a key which can replace the public key infrastructure... The present invention is also particularly useful as it requires a relatively small amount of of computational power to be operative. "

As such, the present invention fulfills a long felt need as the public key infrastructure system requires excessive amounts of computational power. As previously discussed, the present invention is superior to a symmetric key system since the present invention is based on random maps and not based on algorithms and therefore not susceptible to a "brute force attack" (page 30 line 1-2)

In further support for traversing Examiner's rejections under 103(a), Applicant submits with this response a declaration under 37 CFR 1.132 by an Andre Szykier. A CV of Mr. Szykier is further included which shows that he is a mathematian and expert in the field of computer security. Mr Szykier has been engaged as a security expert for business and government agencies. Mr. Szykier has been aware of Applicant's invention and points out many "unexpected results" and "long felt need" arising from Applicant's invention. In particular, the use of "random strings, i.e. maps produced by human action", to create "unbreakable keys" gives rise to "a lightweight and fast encryption with negligible processing requirements".

In view of the above amendments and remarks it is respectfully submitted that independent claims 28 and 47, and dependent claims therefrom are in condition for allowance. Prompt notice of allowance is respectfully and earnestly solicited.

Respectfully submitted,

Mark M. Friedman
Attorney for Applicant
Registration No. 33,883

Date: Feb 6, 2005